RCA 88813

CITED BY APPLICANT

PCT

INTERNATIONALER VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G06F 1/00

A1

(11) Internationale Veröffentlichungsnummer: WO 99/12088

(43) Internationales Veröffentlichungsdatum: 11. März 1999 (11.03.99)

(21) Internationales Aktenzeichen: PCT/DE98/02517

(22) Internationales Anmeldedatum: 27. August 1998 (27.08.98)

(30) Prioritätsdaten:
197 38 325.4 2. September 1997 (02.09.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS NIXDORF INFORMATIONSSYSTEME AG [DE/DE]; Heinz–Nixdorf–Ring 1, D–33106 Paderborn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: WIEHLER, Gerhard [DE/DE]; Am Bogen 43, D–82223 Eichenau (DE).

(74) Gemeinsamer Vertreter: SIEMENS NIXDORF INFORMATIONSSYSTEME AG; Epping, Wilhelm, Postfach 22 13 17, D–80503 München (DE).

(81) Bestimmungsstaaten: AU, CA, CN, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR CONTROLLING DISTRIBUTION AND USE OF SOFTWARE PRODUCTS WITH NETWORK–CONNECTED COMPUTERS

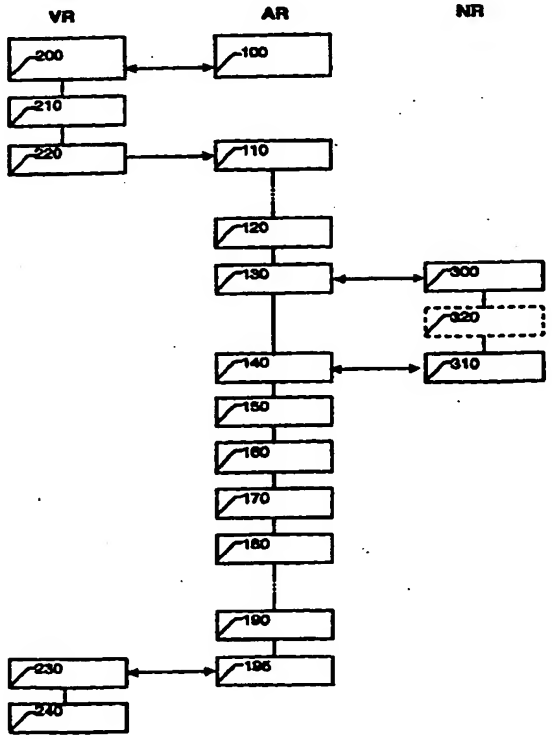
(54) Bezeichnung: VERFAHREN ZUR STEUERUNG DER VERTEILUNG UND NUTZUNG VON SOFTWARE–OBJEKTEN BEI VERNETZTEN RECHNERN

(57) Abstract

The distribution is controlled by means of central certificates acting as a link between the authorizations granted to various users and the right–of–access code allocated to the software products in connection with a special separated control program. The certificates are issued to users on request and intended for calling the wanted software products. Such certificates can be supplemented with distinct control functions. Said functions are executed by the control program, which is supplemented accordingly, especially for recording data on the utilization volume. The invention also relates to the following items: key safety, use of a chip card, integrated copy protection.

(57) Zusammenfassung

Die Verteilung wird durch zentrale Zertifikate als Bindeglied zwischen den den einzelnen Nutzern zugeteilten Berechtigungen und den den Software–Objekten zugeordneten Berechtigungskennzeichen in Verbindung mit einem gesonderten Steuerprogramm gesteuert. Die Zertifikate werden den Nutzern auf Anforderung zugestellt und dienen zum Abruf der gewünschten Software–Objekte. Zertifikate können durch gesonderte Steuerfunktionen ergänzt werden, die vom entsprechend ergänzten Steuerprogramm ausgeführt werden, so zum Beispiel für eine Erfassung von Daten über den Nutzungsumfang. Weiterhin: Sicherung über Schlüssel, Verwendung einer Chipkarte, integrierter Kopierschutz.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren zur Steuerung der Verteilung und Nutzung von Software-Objekten bei vernetzten Rechnern

Die Erfindung betrifft ein Verfahren für Datennetze, bei denen Datensammlungen oder Programme als Software-Objekte an zentraler Stelle verwaltet und auf Anforderung von mit dem Datennetz gekoppelten Rechnern über das Datennetz vorübergehend dem jeweils anfordernden Rechner zur Nutzung zur Verfügung gestellt werden, wobei die Nutzung an den Nutzern zugeteilte Berechtigungen gekoppelt ist.

Über Datennetze können Datenbänke angesteuert und dortige Datensammlungen abgefragt werden. Auch Programme können über Datentnetze den angeschlossenen Rechnern auf Anforderung zur Verfügung gestellt werden. In beiden Fällen bietet die zentrale Verwaltung derartiger Software-Objekte den Vorteil, daß immer der neueste Informationsstand oder die neueste Programmversion verfügbar ist. Der Zugriff ist meistens an entsprechende Berechtigungen gebunden, die mit Bezug auf die einzelnen Software-Objekte sehr unterschiedlich sein können. Auch sind für die Nutzung der Software-Objekte vielfach Gebühren zu entrichten, so daß eine Erfassung des Nutzungsumfanges notwendig ist.

Aufgabe der Erfindung ist es, die in Verbindung mit einer zentralen Verwaltung von Software-Objekten gegebenen Probleme der Zugangsberechtigung und der Nutzungserfassung günstig zu lösen und dabei im gesamten Datennetz eine einheitliche und flexibel anpaßbare Verteilung und Nutzung zu ermöglichen, die den verschiedensten Anforderungen gerecht wird.

Ausgangspunkt für eine derartige Lösung ist das durch die Merkmale des Patentanspruches 1 gekennzeichnete Verfahren. Danach wird der Zugang zu den Software-Objekten durch zentral erstellte, benutzerspezifische Zertifikate in Verbindung mit

einem gesonderten Steuerprogramm geregelt. Durch die damit gegebene zentrale Verwaltung der Nutzungsrechte kann sehr flexibel auf Änderungen von Zugriffsrechten der Nutzer reagiert und netzweit ein einheitlicher Verteilungsmechanismus verwendet werden.

Die Zertifikate und das gesonderte Steuerprogramm eröffnen außerdem die Möglichkeit, weitere Funktionen in einheitlicher Weise zu realisieren, indem diese durch weitere Steuerparameter bzw. entsprechende Programmfunktionen ergänzt werden. So kann entsprechend einer Weiterbildung während eines Programmlaufs ein weiteres Software-Objekt automatisch angefordert und nachgeladen werden, wenn sich eines der vorliegenden Zertifikate auf dieses weitere Software-Objekt bezieht.

Weiterhin in einfacher Weise durch das ergänzte gesonderte Steuerprogramm die Erfassung des Nutzungsumfanges abhängig von entsprechenden Angaben im Zertifikat gesteuert werden, wobei verschiedene Möglichkeiten der Erfassung gegeben sind.

Eine weitere vorteilhafte Ausgestaltung ergibt sich durch die Meldung der Daten über die Nutzungserfassung an eine zentrale Verwaltungsinstanz im Netz, so daß jederzeit Auskunft über die eingesetzten Software-Objekte und deren Nutzungsumfang gegeben werden kann. Der Zeitpunkt und der Umfang der Meldung kann unterschiedlich so gestaltet werden, daß die Rückmeldung nach Ablauf der Gültigkeitsdauer eines Zertifikats erfolgt und die zu diesem gehörigen objektbezogenen Erfassungsdaten umfaßt oder die Rückmeldung nach Ablauf der Gültigkeitsdauer für das gesonderte Steuerprogramm erfolgt und alle vorliegenden Erfassungsdaten umfaßt.

Das Verfahren kann auch auf Netze mit mehreren eigenständigen Verwaltungsinstanzen für Software-Objekte ausgedehnt werden.

Ein weiterer Vorteil besteht darin, daß das Verfahren mit verschiedenen Sicherheitsstandards arbeiten kann. Zweckmäßig

ist es, wenn alle Verbindungsherstellungen im Datennetz und Übertragungen durch Schlüssel gesichert erfolgen, die zweckmäßig auf einer benutzerbezogenen Chipkarte gespeichert sind. Die Verwendung einer Chipkarte als Datenträger bindet den Nutzer auch nicht an einen lokalen Arbeitsplatz, er kann vielmehr von jedem Rechner im Netz aus tätig werden. Dabei wird die Chipkarte zweckmäßig auch für die Erfassung der Daten über den Nutzungsumfang verwendet.

Weiterhin kann der Kopierschutz von Software-Objekten in einfacher Weise durch entsprechende Ergänzung der zugehörigen Zertifikate und des gesonderten Steuerprogramms sichergestellt werden.

Weiterhin kann der das Steuerprogramm überprüfen, ob angeforderte Software-Objekte bereits auf dem anfordernden Rechner verfügbar ist und bei positivem Ergebnis die lokale Bereitstellung des Software-Objektes veranlassen. Die mehrmalige Übertragung des Software-Objekte zum Rechner kann so unterbleiben und die Performance erhöht werden.

Insgesamt ermöglicht die Erfindung bei zentraler Software- und Rechte-Verwaltung eine dezentrale Software-Nutzung. Sie basiert auf Technologien, welche skalierbare Sicherheit gewährleisten und höchste Sicherheitsanforderungen erfüllen können. Auch löst die Erfindung die Verteilung und Nutzungserfassung gültiger Software-Versionen sowie die Löschung nicht mehr benötigter Versionen weitgehend automatisch. Eine Auskunft über die eingesetzten Software-Objekte sowie über ihre Nutzung ist jederzeit möglich. Eine netzweite Erfassung der Daten über den Nutzungsumfang kann periodisch durchgeführt werden und ist parametrisierbar, z. B. monatlich. Nutzer können Software auf beliebige am Netz angeschlossene Rechner laden und anwenden. Eine zentrale Verwaltung ermöglicht die netzweite Einhaltung von Verteilungs- und Nutzungsregeln. Gleichwohl kann dem Nutzer die Freiheit gewährt wer-

den, Einstellungen entsprechend der individuellen Gegebenheiten seines Arbeitsplatzes vorzunehmen.

Einzelheiten der Erfindung seien nachfolgend anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert. Im einzelnen zeigen

FIG 1 ein Übersichtsschema der für die Durchführung des Verfahrens gemäß der Erfindung benötigten Netzwerkkomponenten,

FIG 2 eine schematische Darstellung einer mit verschiedenen Schlüsseln und Programmen geladenen Chipkarte und

FIG 3 ein Ablaufdiagramm des Verfahrens gemäß derErfindung.

FIG 1 zeigt ein Netzwerk mit beispielsweise einem von mehreren Arbeitsplatzrechnern AR, der zur Nutzung aus dem Netz geladener Software verwendet wird, einer Chipkarte 10, die ein Nutzer zur Authentisierung und zum Nachweis entsprechender Software-Nutzungsberechtigungen verwendet, einem zentralen Verwaltungsrechner VR, auf dem sämtliche Software-Objekte und Software-Nutzungsberechtigungen administriert werden, und einem beliebigen Netzrechner NR , auf dem Software-Objekte gespeichert sind, die bei Anforderung auf den Arbeitsplatzrechner AR geladen werden können. Die Rechner sind über ein übliches Datenkommunikationsnetz 30 - zweckmäßigerweise über ein Internet oder Intranet - miteinander verbunden. Verwaltungsrechner VR und Netzrechner NR sind zwar logisch getrennt dargestellt, sie können aber auf derselben Hardwareplattform installiert sein.

Der Verwaltungsrechner VR enthält z. B. ein Software-Administrationsprogramm 41, im folgenden SOA-Programm genannt, ein Programm zur Erfassung der Software-Nutzungsdaten 42, im folgenden SUC-Programm genannt, ein Programm zur Administration der Software Nutzungsrechte sämtlicher Nutzer im Netz 43, im folgenden USAR-Programm genannt, und ein Programm

zur Ausstellung von Zertifikaten zum Zwecke der Software-Nutzung 44, im folgenden ISC-Programm genannt.

Das SOA-Programm 41 kann auf existierenden Produkten, z. B. SMS von Microsoft, basieren, die aber gegebenenfalls erweitert werden müssen. Es administriert eine Datenbank 45 der im Netz verfügbaren Software-Objekte. In der Software-Objekt-Datenbank werden relevante Informationen und Eigenschaften der einzelnen Objekte geführt ,z. B. Hersteller, Versions-Nr., Größe, Location im Netz, Kopierschutz,usw. In dieser oder in einer separaten Datenbank wird je Objekt ein Rollenkennzeichen geführt, das angibt, welchen Rollen im Unternehmen Zugriff auf das jeweilige Software-Objekt erlaubt ist. Typische Rollen im Unternehmen können z. B. sein: Software-Engineer, Marketing-Direktor, Executive-Manager. Der Inhalt der Software-Objekt-Datenbank kann z. B. nach den Spezifikationen des Security Modells von Microsoft vorgenommen werden.

Das SUC-Programm 42 führt in einer Datenbank 46 dynamisch die Software-Nutzungsdaten, d.h. den aktuellen Stand der auf allen Arbeitsplatzrechnern AR genutzten Software. Aktuelle Daten können hier jederzeit abgefragt werden.

Mittels des USAR-Programms 43 werden in einer Datenbank 47 die relevanten Rollen sowie die Zuordnung zu sämtlichen Nutzern im Netz definiert und verwaltet. Jedem Nutzer können eine oder mehrere Rollen zugewiesen werden. Die Anzahl der Rollen ist beliebig erweiterbar.

Das ISC-Programm 44 stellt den Nutzern auf Anforderung sogenannte „User Software Certificates" USC zur Verfügung, durch welche die Berechtigung zur Nutzung von Software erteilt wird. Zur Ausstellung der Zertifikate USC benötigt das ISC-Programm 44 Zugriff auf die Datenbänke 47 und 45.

Die Kommunikation zwischen dem Verwaltungsrechner VR und den Arbeitsplatzrechnern erfolgt zweckmäßigerweise über einen

WWW-fähigen Server 48, z. B. Microsofts Internet Information Server oder Netscape's Internet Server. Die Programme 41, 42, 43, und 44 können beispielsweise als Backend-Applikationen über sogenannte CGI-Scripts angebunden sein.

Das Administrator-Interface zur Administration der SOA- und USAR-Programme 41 und 43 bzw. das Recherche-Interface für das SUC-Programm 42 kann z. B. ein beliebig im Netz lokalisierter Browser 60 sein.

Auf dem Arbeitsplatzrechner AR ist zweckmäßigerweise ein weiterer Browser 21 installiert, welcher die Kommunikation mit den Rechnern VR und NR abwickelt. Die Software-Komponente 22, im folgenden SCV-Programm genannt, wird bei jeder Anfrage des Arbeitsplatzrechners AR auf Zuteilung von Software-Nutzungsrechten zusammen mit einer sogenannten HTML-Page zweckmäßigerweise mittels Protokoll HTTPS, z. B. als ActiveX Control oder als „Plug in", vom Verwaltungsrechner VR zum Arbeitsplatzrechner AR übertragen. Die HTML-Page stellt als Liste ASL am Bildschirm die erlaubten Zugriffsmöglichkeiten auf Netz-Software dar.

Bei einer Download-Anforderung verifiziert das SCV-Programm mittels der Zertifikate USC die Nutzungs-Berechtigung. Das SCV-Programm steuert desweiteren die Erfassung der Software-Nutzungsdaten, z. B. Anzahl der Downloads, Nutzungszeit einer SW,usw..

Die Programme 24 bis 2x sind z. B. Anwendungsprogramme, die der Nutzer aus dem Netz geladen hat und anwendet.

Die Chipkarte 10 wird über einen üblichen, am Arbeitsplatzrechner AR angeschlossenen Chipkartenleser 23 betrieben. Die Karte entspricht zweckmäßigerweise dem Standard 7816. Vorteilhafter ist aus Sicherheitsgründen eine Chipkarte mit Cryptocontroller, wie z. B. SLE 44CR80S von Siemens, da diese

für offene Netze, wie z. B. das Internet mit auf Public Key-Basis arbeitenden Sicherheitsmechanismen, besonders geeignet.

Chipkartenanwendungen und Chipkartenleser können z. B. im Arbeitsplatzrechner AR entsprechend den von der „PC/SC Workgroup" festgelegten Spezifikationen und Interfaces, unterstützt werden. Weitere Information dazu sind unter

http://www.smartcardsys.com.

zu finden.

Jeder Nutzer am Netz erhält eine individuelle Chipkarte. Die Chipkarte wird vor Auslieferung an den Nutzer in einem sogenannten Personalisierungsprozeß, z. B. bei einem Kartenhersteller, mit den persönlichen Daten des Nutzers personalisiert. Mindestens müssen, wie FIG 2 zeigt, ein privater Schlüssel 11a und ein Zertifikat des öffentlichen Schlüssels 11b des Nutzers auf die Karte gespeichert (personalisiert) werden. Der private Schlüssel und das Zertifikat des öffentlichen Schlüssels des Nutzers werden z. B. in einem Trust Center erzeugt und auf sicherem Wege der Personalisierungsstelle zur Verfügung gestellt, wo sie dann in üblichen Verfahren auf die Chipkarte gespeichert werden.

Mittels dieses Schlüssel-Zertifikatspaares 11a/11b und eines entsprechenden Paares auf dem Verwaltungsrechner VR kann nach heute üblichen Verfahren, z. B. SSL V3.0, eine beidseitige und sichere Client/Server-Authentisierung durchgeführt werden. Dies ist die Voraussetzung für die sichere Übertragung von Zertifikaten USC, die der Nutzer zur Nutzung von Software benötigt.

Je nach Sicherheitsanforderungen können weitere Schlüssel-Zertifikatspaare 12a/12b - z. B. für einen Intergritätsschutz von Zertifikaten USC oder die sichere Kommunikation zwischen Programmen auf dem Verwaltungsrechner VR und dem Arbeitsrech-

ner AR oder für das Nachladen von Schlüsseln oder Anwendungen auf die Karte über das Netz - auf die Chipkarte personalisiert bzw. im Netzbetrieb nachträglich mittels sicherer Verfahren auf die Chipkarte geladen werden.

Bereits bei der Personalisierung oder ebenfalls im Netzbetrieb werden Applikationsprogramme 13a bis 13x auf die Chipkarte geladen, die der Erfassung der Software-Nutzung, z. B. Anzahl der Downloads oder Zeiterfassung, dienen.

Anhand von FIG 3 wird das Verfahren des Software-Downloads, der Software-Nutzung und der Nutzungserfassung erläutert. Folgende Verfahrensschritte werden dabei ausgeführt:

100: Der Nutzer meldet sich beim Verwaltungsrechner VR an und authentisiert sich mittels des üblichen HTTPS-Protokoll im SSL-Dialog unter Verwendung seines privaten Schlüssels auf der Chipkarte.

200: Der Verwaltungsrechner VR authentisiert sich ebenfalls und identifiziert den Nutzer.

210: Der Verwaltungsrechner VR stellt unter Auswertung der Datenbänke 45 und 47 die Inhalte der nutzerspezifischen Zertifikate USC bereit.Dabei werden Zertifikate für jene Software-Objekte erstellt, deren Rollenkennzeichen mit einer oder mehreren Rollen, die der Nutzer besitzt, übereinstimmt.
Ein Zertifikat USC kann z. B. enthalten: Software-ID, Versions-Nr., Location im Netz, Größe des Software-Objekts, Art der Nutzungserfassung, Zeitintervall der Erfassungsmeldung an den VR, Löschungsmodus, Gültigkeitsdauer des USC, ID des ausstellenden Verwaltungsrechners VR.
Bei der Art der Nutzungserfassung können z. B. folgende Parameter Verwendung finden: Erfassung der Download-Anzahl, Erfassung der aktiven Nutzungszeit, keine Erfassung.

220: Die bereitgestellten Zertifikate USC werden mit dem Public Key des Nutzers im Verwaltungsrechner VR integritätsgeschützt, gegebenenfalls auch zusätzlich mit im Internet üblichen Verfahren verschlüsselt,) und eingebunden in die HTML-Page ASL zusammen mit dem SCV-Programm 22 an den Arbeitsplatzrechner AR übertragen.
Da das SCV-Programm im Arbeitsplatzrechner AR sicherheitsrelevante Funktionen ausführt, sollte es zweckmäßig mit einer digitalen Signatur des Verwaltungsrechner VR versehen sein.

110: Im Arbeitsplatzrechner AR erscheint die HTML-Page ASL auf dem Bildschirm. Sie zeigt alle dem Nutzer zugänglichen Software-Objekte an.
Implizit ist eine Gültigkeitsdauer in der HTML-Page enthalten, nach deren Ablauf sich die Page samt des SCV-Programm und der Zertifikate USC zerstören. Für die Dauer der Gültigkeit wird sie im Browser verfügbar gehalten und kann nach jedem Einschalten des Arbeitsplatzrechners AR ohne Kommunikation mit dem Verwaltungsrechner VR aufgerufen werden. Nach jedem Aufruf des SCV-Programms kann vorzugsweise eine Verifikation der digitalen Signatur erfolgen, um Manipulationen zu vermeiden bzw. zu entdecken.

120: Der Nutzer kann nun die zum Download gewünschten Software-Objekte anklicken. Dadurch wird automatisch das SCV-Programm gestartet. Das SCV-Programm und die betreffenden Zertifikate USC werden daraufhin unter Verwendung der auf der Chipkarte befindlichen Schlüssel verifiziert.

130: Nach positiver Verifizierung ermittelt das SCV-Programm die Netzrechner-Adresse(n) aus dem(n) Zertifikaten USC und stellt die WWW-Verbindung zum ersten Netzrechner NR her. (Nach abgeschlossenem Download gegebenenfalls auch zu weiteren Netzrechnern NR.)

130/300: Es erfolgt die gegenseitige Authentisierung zwischen Arbeitsplatzrechner AR und Netzrechner NR entsprechend einem üblichem Verfahren.

310/140: Danach kann das Programm 51 das (die) gewünschte(n) Software-Objekt(e) selektieren und an den Arbeitsplatzrechner AR senden.

320: Zur Erhöhung der Sicherheit, insbesondere bei Anwendung des Verfahrens im Internet, kann es sinnvoll sein, im Netzrechner NR ebenfalls eine Verifizierung der Zertifikate USC mittels des Programms 53 nach üblichen Verfahren vorzunehmen. Beispielsweise werden die Zertifikate USC im Arbeitsplatzrechner AR mit dem Private Key des Nutzers signiert und im Netzrechner NR mit seinem Public Key verifiziert. In diesem Fall würde die Freigabe des angeforderten Software-Objekts aus der Objektdatenbank 52 erst nach positiver Verifikation erfolgen, wie gestrichelt angedeutet.

Eine weitere Erhöhung der Sicherheit kann dadurch erreicht werden, daß das zu übertragende Software-Objekt im Netzrechner NR mit einer digitalen Signatur versehen wird und im Arbeitsplatzrechner AR vor Nutzung eine Verifikation erfolgt. Damit könnte eine Verfälschung des Objektes bei der Netzübertragung entdeckt werden.

150: Im nächsten Schritt stellt auf dem Arbeitsplatzrechner AR das SCV-Programm 22 anhand der USC-Parameter die Art der Nutzungserfassung fest und wird entsprechend tätig. Beispielsweise wird, wenn der Parameter „Erfassung der Anzahl von Downloads" gesetzt ist, eine objektbezogene Zähleranwendung auf der Chipkarte, z. B. 13a in FIG 2, aktiviert und der Zähler erhöht. Zählvorgänge auf der Chipkarte werden zweckmäßig in üblicher Weise kryptographisch abgesichert durchgeführt.

160: Der Nutzer erkennt nach dem Download an Hand der Liste ASL auf dem Bildschirm, welche Software lokal vorhanden ist, und kann den Start per Klick auslösen.

170: Dadurch wird gleichzeitig - falls ein dementsprechender USC-Parameter gesetzt ist - die Nutzungszeiterfassung durch das SCV ausgelöst und die Nutzungszeit während der aktiven Nutzung periodisch erfaßt, indem das SCV-Programm 22 einen objektbezogenen Zeitzähler auf der

Chipkarte, z. B. 13b in FIG 2, von Zeit zu Zeit (parametrisierbar) erhöht.

180: Nach Beendigung der Nutzung eines geladenen Software-Objektes auf dem Arbeitsplatzrechner AR entscheidet das SCV-Programm 22 anhand des Löschungsmodus-Parameters, ob das Programm gelöscht oder im Arbeitsplatzrechner AR gespeichert wird.

190: Eine Nutzungserfassungs-Rückmeldung an den VR wird entweder durch Ablauf des Zeitintervall-Parameters eines Zertifikats USC oder durch Ablauf eines Zeitintervalls im SCV-Programm 22 ausgelöst. Im Falle der Zertifikats-Auslösung sind nur die zum betreffenden Zertifikat USC gehörenden objektbezogenen Erfassungsdaten betroffen, im SCV-Auslösungsfall die Erfassungsdaten sämtlicher Zertifikate USC. Entsprechend werden die zugehörigen Download-Zähler und Nutzungszeitzähler aus der Chipkarte 10 ausgewählt.

195/230: Nach der üblichen gegenseitigen Authentisierung zwischen Arbeitsplatzrechner AR und Verwaltungsrechner VR werden die ausgewählten Zählerstände an den Verwaltungsrechner VRübertragen.

240: Im Verwaltungsrechner VR werden die entsprechenden Erfassungsdaten mittels des SUC-Programms 42 ausgewertet und in die Datenbank 46 eingetragen.

Bei Ziehen der Chipkarte erscheint z. B. eine Dialogbox mit der Warnung, daß das Programm nach einer bestimmten Zeit (parametrisierbar) gelöscht wird, wenn die Karte nicht wieder eingeführt wird.

Das beschriebene Verfahren ermöglicht durch die zentrale Verwaltung der Nutzungsrechte und Nutzungserfassungsparameter im Verwaltungsrechner VR eine netzweit einheitliche und flexibel anpaßbare Software-Verteilung und -Nutzung. Gleichwohl kann der Nutzer einzelne Parameter ändern oder selbst bestimmen, falls ein entsprechender USC-Parameter diesen Freiheitsgrad

erlaubt. Z. B. kann der Nutzer das Löschen oder Speichern eines Programms nach Nutzung selbst entscheiden.

Im Falle der Änderung einzelner USC-Parameter durch den Nutzer bleibt das ursprünglich integritätsgeschützte Zertifikat USC unverändert, wodurch gewährleistet wird, daß bei wiederholten Downloads jeweils eine Integritäts-Verifikation durchgeführt werden kann.

Die Funktionalität kann dadurch erweitert werden, daß ein automatischer Download durch das SCV-Programm 22 für den Fall ausgelöst wird, wenn ein Software-Objekt zur Laufzeit ein anderes Software-Objekt aufruft, z. B. OLE-Technik, das nicht auf dem Arbeitsplatzrechner AR verfügbar ist, dessen Identität aber in einem der Zertifikate USC festgestellt werden kann.

Der Nutzer in einem Netzwerk kann das Verfahren von beliebigen am Netz angeschlossenen Rechnern aus anwenden, wenn er jeweils seine individuelle Berechtigungs- und Erfassungs-Chipkarte an diesem Rechner betreiben kann. Bei einem Rechnerwechsel muß er lediglich vor dem ersten Download eines Software-Objektes mit dem Verwaltungsrechner VR kommunizieren, um sich die aktuellen Rechte entsprechend dem oben beschriebenen Verfahren erteilen zu lassen.

Bei fortschreitender Chipkarten-Technologie kann die HTML-Page mit der Liste ASL und das SCV-Programm auf der Chipkarte gespeichert sein und zum Ablauf gebracht werden. In diesem Fall entfällt bei Rechnerwechsel die Kommunikation mit dem VR.

Aus Sicht des Nutzers läßt sich das Verfahren auch auf verschiedene, voneinander unabhängige Netze anwenden, z. B. Intranet für Rechte innerhalb der eigenen Firma, Extranet für Rechner in einer Partnerfirma, Internet für Rechte zur welt-

weiten Nutzung. Das kann mit ein und derselben oder mit separaten Chipkarten erfolgen. Bei Verwendung derselben Chipkarte müssen separate Schlüssel für die verschiedenen Verwaltungsrechner VR zur Verfügung stehen.

Eine Erweiterung des Verfahrens ist auch dadurch möglich, daß Mechanismen zum Kopierschutz in das beschriebene Verfahren einbezogen werden. Hierzu wird für Software-Objekte, die kopiergeschützt sein sollen, unter Verwendung des Public Key des Nutzers eine sog. „Key File" erzeugt, die der Nutzer nach dem Download des Software-Objekts erhält. Nur mit dieser „Key File" und unter Verwendung des Private Key des Nutzers kann das Software-Objekt genutzt werden.

Durch Festlegung eines USC-Parameters „kopiergeschützt" und Erweiterung der Funktionen des SCV-Programms für die erforderliche Kommunikation zwischen Arbeitsplatzrechner AR und Verwaltungsrechner NR sowie Arbeitsplatzrechner AR und Chipkarte 10 entsprechend der für den Kopierschutz festgelegten Verfahren, läßt sich der Kopierschutz einfach in das hier erläuterte Verfahren integrieren.

Für das Verfahren können außerdem multifunktionale Chipkarten verwendet werden, die z. B. auch für andere Netzanwendungen eingesetzt werden. Vorzugsweise ist eine Kombination mit Anwendungen zur Identifikation im Netz sinnvoll. Solche Anwendungen könnten z. B. sein: WWW-Client Authentifikation gegenüber einem Internet Server, WWW-Client Identifikation bei Mail (z. B. S/MIME), WWW-Client Identifikation zur Gewährung von Zugriffsrechten auf Netzressourcen.

Das Verfahren kann generell auch - bei geringeren Sicherheitsanforderungen - ohne die Verwendung von Chipkarten angewandt werden. Die auf der Chipkarte befindlichen Schlüssel und Zähler können z. B. auch auf einer Diskette (z. B. mit einem Paßwort verschlüsselt) geführt werden, und die auf der

Chipkarte durchgeführten Operationen könnte das SCV-Programm 22 übernehmen.

5

Patentansprüche

1. Verfahren zur Steuerung der Verteilung und Nutzung von als Software-Objekte bezeichnete Datensammlungen oder Programme bei über ein Datennetz (30) gekoppelten Rechnern (AR) an zentraler Stelle (NR) verwaltet und auf Anforderung vorübergehend dem jeweils anfordernden Rechner (AR) zur Nutzung zur Verfügung gestellt werden, wobei

- die Nutzungsrechte in Form von benutzerspezifischen Zertifikaten (USC) ausgebildet sind, die als Bindeglied zwischen den den einzelnen Benutzern zugeteilten Berechtigungen und den Software-Objekten zugeordneten Berechtigungskennzeichen erstellt werden;
- bei jeder Anfrage nach einem Software-Objekt an eine zentrale Verwaltungsinstanz (VR) die Zertifikate (USC) jeweils nutzerbezogen an den anfordernden Rechner (AR) übertragen werden;
- die Zertifikate (USC) vor der Nutzung der Software-Objekte mittels eines persönlichen Datenträgers (10) verifiziert werden und die Nutzung auf dem selben Datenträger (10) erfaßt wird;
- ein gesondertertes Steuerprogramm (SCV-Programm 22) im anfordernden Rechnern (AR) auf Basis der Nutzungsrechte die das Software-Objekt betreffenden Aktionen steuert und Statusmeldungen an die zentrale Stelle (NR) meldet.

2. Verfahren nach Anspruch 1, bei dem das Steuerprogramm (SCV) von der zentralen Stelle (NR) zum anfordernden Rechner (AR) übertragen wird und vor seiner Nutzung mittels des persönlichen Datenträgers (10) verifiziert wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem die benutzerspezifischen Zertifikate (USC) auf dem als Chipkarte ausgebildeten Datenträger (10) gespeichert werden.

4. Verfahren nach Anspruch 3, bei dem das Steuerprogramm (SCV) im Datenträger (10) residiert und zumindest teilweise dort ausgeführt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem der Datenträger (10) mit beliebigen Rechnern (AR) des Datennetz (30) gekoppelt werden kann.

6. Verfahren nach einem der Ansprüche 1 bis 5, bei dem das Steuerprogramm (SCV) überprüft ob angeforderte Software-Objekte bereits auf dem Rechner (AR) verfügbar ist und bei positivem Ergebnis die lokale Bereitstellung des Software-Objektes veranlaßt.

7. Verfahren nach einem der Ansprüche 1 bis 6, bei dem nach Übertragung der Zertifikate (USC) ein Verzeichnis der den Zertifikaten entsprechenden Software-Objekte auf dem Bildschirm des anfordernden Rechners (AR) dargestellt wird und die Anforderung für das jeweils gewünschte Software-Objekt durch den Nutzer ausgelöst wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, bei dem die Bereitstellung der Software-Objekte durch verschiedene Rechner (NR) im Netz (30) erfolgen kann.

9. Verfahren nach einem der Ansprüche 1 bis 8, bei dem in den Zertifikaten (USC) enthaltene Steuerparameter durch den Nutzer änderbar sind, ohne daß ein bestehender Integritätsschutz verloren geht.

10. Verfahren nach einem der Ansprüche 1 bis 9, bei dem ein während der Laufzeit eines Programms als Software-Objekt aufgerufenes weiteres Programm, das in einem der vorliegenden Zertifikate (USC) bezeichnet ist, automatisch durch das gesonderte Steuerprogramm (22) angefordert und daraufhin an den die Anforderung stellenden Rechner (AR) übertragen wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, bei dem die Löschung von Software-Objekten automatisch bei Beendigung ihrer Nutzung erfolgt.

12. Verfahren nach einem der Ansprüche 1 bis 11, bei dem die Zertifikate (USC) Angaben über die Art der Erfassung des Nutzungsumfanges der an einen anfordernden Rechner (AR) übertragenen Software-Objekte enthalten und daß das gesonderte Steuerprogramm (22) auf Grund dieser Angaben die Erfassung des Nutzungsumfanges steuert.

13. Verfahren nach Anspruch 12, bei dem der Nutzungsumfang durch Zählung der übertragenen Software-Objekte erfolgt.

14. Verfahren nach Anspruch 12,
dadurch gekennzeichnet,
daß der Nutzungsumfang durch Zählung von periodisch wiederkehrenden Taktimpulsen erfolgt.

15. Verfahren nach einem der Ansprüche 12 bis 14, bei dem die Erfassung der Daten über den Nutzungsumfang auf dem Datenträger (10) erfolgt.

16. Verfahren nach einem der Ansprüche 1 bis 15, bei dem in Datennetzen (30) mit mehreren unabhängigen Verwaltungsinstanzen (VR) für Software-Objekte jede Verwaltungsinstanz Nutzungszertifikate (USC) für die zu ihrem Zuständigkeitsbereich gehörenden Software-Objekte erstellt.

17. Verfahren nach einem der Ansprüche 1 bis 16, bei dem alle Verbindungsherstellungen im Datennetz (30) und Übertragungen durch Schlüssel gesichert erfolgen.

18. Verfahren nach Anspruch 17, bei dem die Schlüssel auf dem Datenträger (10) enthalten sind.

19. Verfahren nach einem der Ansprüche 1 bis 18, dadurch gekennzeichnet, daß dem Kopierschutz unterliegende Software-Objekte durch zusätzliche Steuerparameter im zugehörigen Zertifikat (USC) und entsprechende Steuerfunktionen im gesonderten Steuerprogramm (22) gegen ein Kopieren gesichert werden.

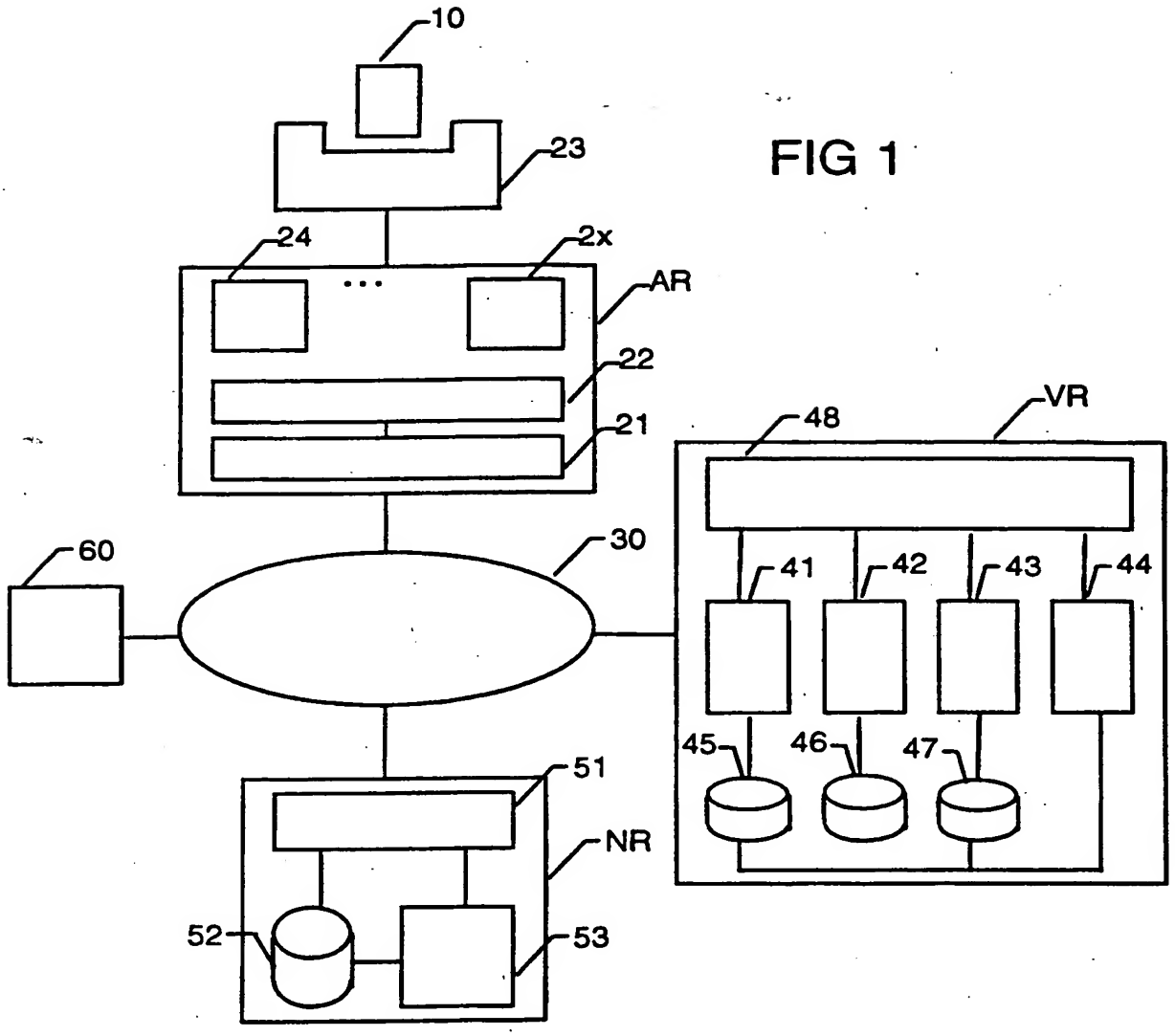

10
23
24
2x
AR
22
21
VR
48
60
30
41
42
43
44
45
46
47
51
NR
52
53

FIG 1

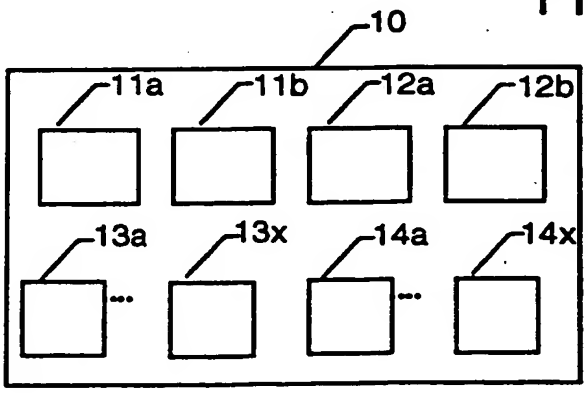
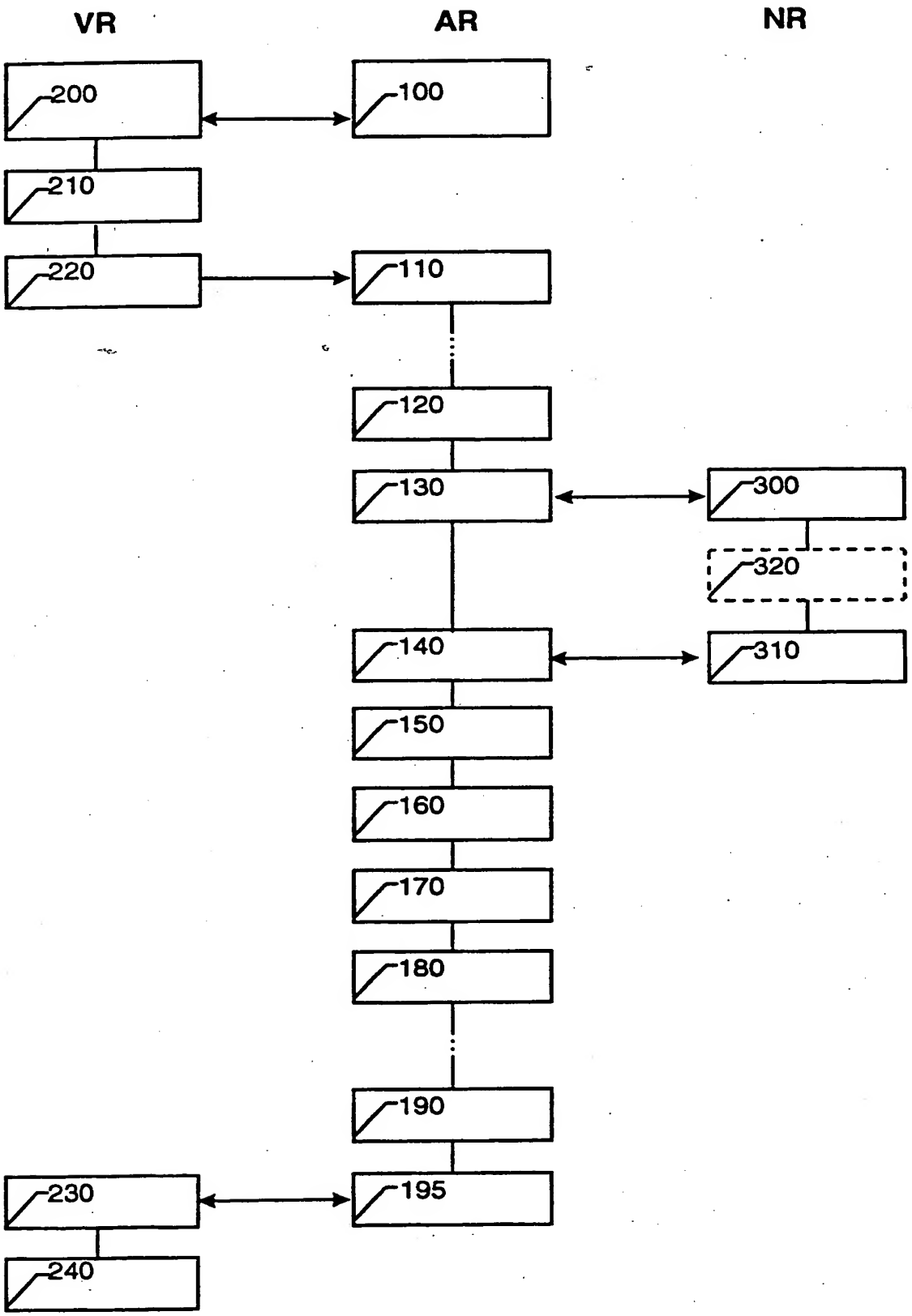

10
11a
11b
12a
12b
13a
13x
14a
14x

FIG 2

FIG 3


VR
AR
NR
200
100
210
220
110
120
130
300
320
140
310
150
160
170
180
190
230
195
240

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/DE 98/02517

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 421 409 A (IBM) 10 April 1991 see figures 2,5-9,13,14 see page 3, line 35 - page 4, line 29 see page 6, line 18 - page 8, line 27 see page 9, line 53 - page 11, line 26	1-9,12, 17-19
A	WO 95 05050 A (TECHNOLOGY INC B V) 16 February 1995 see figures 1,3,4,6 see page 13, line 29 - page 17, line 9 see page 18, line 35 - page 21, line 3	1,2, 6-13,16, 17,19

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 1999	25/01/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ational Application No
PCT/DE 98/02517

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0421409 A	10-04-1991	US 5048085 A	10-09-1991
		CA 2026739 A,C	07-04-1991
		JP 3237551 A	23-10-1991
		US 5148481 A	15-09-1992
WO 9505050 A	16-02-1995	US 5418713 A	23-05-1995
		AU 7519994 A	28-02-1995
		CA 2192814 A	16-02-1995
		EP 0716795 A	19-06-1996
		US 5794217 A	11-08-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/02517

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 421 409 A (IBM) 10. April 1991 siehe Abbildungen 2,5-9,13,14 siehe Seite 3, Zeile 35 - Seite 4, Zeile 29 siehe Seite 6, Zeile 18 - Seite 8, Zeile 27 siehe Seite 9, Zeile 53 - Seite 11, Zeile 26 ---	1-9,12, 17-19
A	WO 95 05050 A (TECHNOLOGY INC B V) 16. Februar 1995 siehe Abbildungen 1,3,4,6 siehe Seite 13, Zeile 29 - Seite 17, Zeile 9 siehe Seite 18, Zeile 35 - Seite 21, Zeile 3 -----	1,2, 6-13,16, 17,19

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
18. Januar 1999	25/01/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Int. ionales Aktenzeichen
PCT/DE 98/02517

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0421409 A	10-04-1991	US	5048085 A	10-09-1991
		CA	2026739 A,C	07-04-1991
		JP	3237551 A	23-10-1991
		US	5148481 A	15-09-1992
WO 9505050 A	16-02-1995	US	5418713 A	23-05-1995
		AU	7519994 A	28-02-1995
		CA	2192814 A	16-02-1995
		EP	0716795 A	19-06-1996
		US	5794217 A	11-08-1998

Specification

Method for controlling the distribution and utilization of software objects with networked computers.

The invention relates to a method for data networks, in which data collections or programs are administered as software objects at a central location and, upon request by computers coupled with the data network, are made temporarily available via the data network to the particular requesting computer, wherein the utilization is tied to authorizations allocated to the users.

Data bases can be addressed via data networks and data collections there can be queried. Programs can also be made available upon request via data networks to the connected computers. In both cases, the central administration of such software objects offers the advantage that the most recent information status or the most recent program version is always available. Access is most often tied to corresponding authorizations, which, with respect to the discrete software objects, can differ widely. For utilizing the software objects, fees must often be paid such that it is necessary to determine the extent of usage.

It is the task of the invention to solve favorably the problems arising in connection with a central administration of software objects, of access authorization and of the utilization determination and therein make possible over the entire data network the uniform and flexibly adaptable distribution and utilization, which does justice to highly diverse requirements.

Starting point for such a solution is the method characterized by the characteristics of patent claim 1. Accordingly, access to the software objects is controlled by centrally prepared certificates specific to each user in connection with a separate control program. Through the central administration given thereby of the rights of use it is

possible to respond highly flexibly to changes of access rights of the user and a network-wide uniform distribution mechanism can be applied.

The certificates and the separate control program moreover open the feasibility of realizing further functions in a uniform manner, thereby that these are supplemented by further control parameters or corresponding program functions. Thus, according to a further development during one program run a further software object can automatically be requested and reloaded, if one of the present certificates relates to this further software object.

Furthermore, it is possible to control in simple manner through the supplemented separate control program the determination of the extent of use, wherein various feasibilities of acquisition are given.

A further advantageous implementation is obtained through the report of the data about the usage acquisition to a central administrative instance in the network, such that at any time information can be provided about the software objects utilized and the extent of their utilization. The point in time and the extent of the report can be implemented in different ways such that the feedback takes place after the expiration of the validity of a certificate and comprises the object-related acquisition data belonging to it or the feedback occurs after expiration of the validity for the separate control program and comprises all of the available acquisition data.

The method can also be extended to networks with several independent administrative instances for software objects.

A further advantage comprises that the method can operate with different security standards. It is useful if the establishments of all connections in the data network and transmissions take place secured by keys, which usefully are stored on a user-related chip card. The use of a chip card as a data medium does not tie the user to a local work station, rather he can become active using any computer in the network.

The chip card is therein usefully also applied for the acquisition of the data relating to the extent of usage.

The copy protection of software objects can, moreover, be ensured in simple manner through corresponding supplementation of the associated certificates and the separate control program.

Moreover, the control program can check whether or not requested software objects are already available on the requesting computer and, in the event the result is positive, can initiate the local provision of the software object. Repeated transmission of the software object to the computer can thus be omitted and the performance can be enhanced.

Overall, the invention makes possible in a central software and right administration the decentralized software utilization. It is based on technologies, which ensure scalable security and can meet highest security requirements. The invention also solves largely automatically the distribution and usage acquisition of valid software versions as well as the deletion of versions no longer required. Information about the software objects used as well as their usage is possible at any time. A network-wide acquisition of the data relating to the extent of usage can be carried out periodically and can be parameterized, for example, monthly. Users can load onto and apply software on any computer connected to the network. The central administration permits the network-wide observation of distribution and utilization rules. Yet, the user can enjoy the freedom of carrying out settings according to the individual conditions of his work station.

In the following, details of the invention will be explained in further detail in conjunction with an embodiment example depicted in the drawing. Therein show

FIG. 1 an overview diagram of the network components required for carrying out the method according to the invention,

FIG. 2 a schematic representation of a chip card loaded with different keys and programs, and

FIG. 3 a flow chart of the method according to the invention.

Figure 1 shows a network with, for example, one of several work station computers AR, which is used for utilizing software downloaded from the network, a chip card 10, which a user uses for authentication and for documentation of corresponding software use authorizations, a central administration computer VR, on which all software objects and software use authorizations are administered, and any network computer NR on which software objects are stored, which can be loaded onto the work station computer AR upon request. The computers are linked via a conventional data communication network 30 - usefully via Internet or Intranet. Administration computer VR and network computer NR are shown logically separated, however, they can be installed on the same hardware platform.

The administration computer VR comprises, for example, a software administration program 41, referred to in the following as SOA program, a program for the acquisition of the software usage data 42, referred to in the following as SUC program, a program for the administration of the software use rights of all users in network 43, in the following referred to as USAR program, and a program for issuing certificates for the purpose of software utilization 44, in the following referred to as ISC program.

The SOA program 41 can be based on existing products, for example SMS by Microsoft, which, however, must, if appropriate, be expanded. It administers a data base 45 of the software objects available in the network. In the software object data base relevant information and properties of the individual objects are carried, for example, manufacturer, version number, size, location in the network, copy protection, etc. In this or in a separate data base for each object a job position identification, which indicates for which job positions in the company access to the

particular software objects is permitted. Typical job positions in the company can be, for example: software engineer, director of marketing, executive manager. The content of the software object data base can be carried out, for example according to the specifications of the Security Model by Microsoft.

The SUC program 42 carries dynamically in a data base 46 the software usage data, i.e. the current status of the software used on all work station computers AR. Current data can here be queried at any time.

By means of the USAR program 43 in a data base 47 are defined and administered the relevant job positions as well as the allocation to all users in the network. To each user can be assigned one or several job positions. The number of job positions is expandable in any desired way.

Upon request the ISC program 44 makes available to the users so-called "user software certificates" USC, through which the authorization for the use of the software is granted. To issue the certificates USC, the ISC program 44 requires access to the data bases 47 and 45.

Communication between the administration computer VR and the work station computers usefully takes place via a www-capable server 48, for example Microsoft's Internet Information Server or Netscape's Internet Server. Programs 41, 42, 43 and 44 can, for example, be acquired as backend applications via so-called CGI scripts.

The administrator interface to the administration of the SOA and USAR programs 41 and 43, or the search interface for the SUC program 42, can, for example, be any browser 60 localized in the network.

On the work station computer AR usefully a further browser 21 is installed which handles the communication with computers VR and NR. The software component

22, in the following referred to as SCV program is transmitted from the administration computer VR to the work station computer AR following each request by the work station computer AR for allocation of software utilization rights together with a so-called html page, usefully by means of protocol https, for example, as activex control or as "plug-in". The html page represents as a list ASL on the screen the permitted access possibilities to the network software.

Upon a download request, the SCV program verifies by means of the certificates USC the rights of use. The SCV program controls furthermore the acquisition of the software usage data, for example, number of downloads, usage time of a software, etc.

Programs 24 to 2x are, for example, application programs, which the user has downloaded from the network and is applying.

The chip card 10 is operated via a conventional chip card reader 23 connected to the work station computer AR. The card corresponds usefully to standard 7816. For reasons of security, a chip card is advantageously one such with cryptocontroller, such as for example SLE 44CR80S by Siemens, since it is especially suitable for open networks, such as for example the Internet, with security mechanisms operating on the basis of public keys.

Chip card applications and chip card readers can be supported, for example in the work station computer AR according to the specifications and interfaces defined by the "PC/SC Work Group". Further information can be found at

http://www.smartcardsys.com.

Each user on the network receives an individual chip card. Before delivery to the user in a so-called personalization process, the chip card is personalized with the

personal data of the user, for example by a card producer. At least, as shown in Figure 2, a private key 11a and a certificate of the public key 11b of the user must be stored (personalized) on the card. The private key and the certificate of the public key of the user are, for example, generated in a trust center and made available in a safe and secured way to the personalization site, where they are subsequently stored on the chip card in conventional processes.

By means of this key certificate pair 11a/11b and a corresponding pair on the administration computer VR, a client/server authentication can be carried out at both ends and securely, according to currently customary processes, for example SSL V3.0. This is the prerequisite for the secure transmission of certificates USC, which the user requires for utilizing software.

Depending on the security requirements, further key certificate pairs 12a/12b - for example for integrity protection of certificates USC or the secure communication between programs on the administration computer VR and the work station computer AR or for the reloading of keys or applications onto the card via the network - can be personalized on the chip card or can subsequently be loaded onto the chip card in network operation by means of secure processes.

In the personalization, or also in network operation, application programs 13a to 13x are loaded onto the chip card, which serves for the acquisition of the software usage, for example number of downloads or time determination.

In conjunction with Figure 3 the process of the software downloads, the software utilization and the usage acquisition will be explained. The following method steps are therein carried out:

100: The user logs onto the administration computer VR and authenticates himself by means of the conventional https protocol in SSL dialog using his private

key on the chip card.

200: The administration computer VR also authenticates itself and identifies the user.

210: The administration computer VR evaluating the data bases 45 and 47, makes available the contents of the user-specific certificates USC. Certificates for those software objects are issued whose job position identification agrees with one or several job positions which describe the user.
A certificate USC can contain, for example: software ID, version no., location in the network, size of the software object, type of usage acquisition, time interval of the acquisition report to the VR, delete mode, period of validity of the USC, ID of the issuing administration computer VR.
In the type of usage acquisition can be used, for example the following parameters: acquisition of the number of downloads, acquisition of the active usage time, no acquisition.

220: The certificates USC made available are integrity protected with the public key of the user in the administration computer VR, if appropriate also additionally encrypted (with the process customarily used in the Internet) and integrated into the html page ASL together with the SCV program 22 transmitted to the work station computer AR together with the SCV program 22.
Since the SCV program in the work station computer AR carries out functions which are relevant to security, it should usefully be provided with a digital signature of the administration computer VR.

110: In the work station computer AR the html page ASL is displayed on the screen. It indicates all software objects accessible to the user.
Implicitly contained in the html page is a duration of validity, after the expiration of which the page together with the SCV program and the

certificates USC are destroyed. For the duration of the validity it is kept available in the browser and can be called up each time the work station computer AR is switched on, without communication with the administration computer VR. After each call-up of the SCV program, a verification of the digital signature can preferably take place in order to avoid or discover manipulations.

120: The user can now click on the software objects desired for download. Thereby the SCV program is automatically started. The SCV program and the particular certificates USC are thereupon verified using the key disposed on the chip card.

130. After positive verification, the SCV program determines the network computer address(es) from the certificate(s) USC and establishes the www connection to the first network computer NR. (After the download is concluded, if appropriate, also to further network computers NR.)

130/300: The mutual authentication takes place between work station computer AR and network computer NR according to a customary process.

310/140: Subsequently program 51 can select the desired software object(s) and send them to the work station computer AR.

320: To increase the security, in particular when applying the method in the Internet, it can be reasonable to carry out in the network computer NR also a verification of the certificates USC by means of program 53 according to customary processes. For example, the certificates USC are signed in the work station computer AR with the private key of the user and verified in the network computer NR with his public key. In this case, the enabling of the requested software object from the object data base 52 only occurs after

positive verification, as indicated in dashed lines.
A further increase of the security can be attained thereby that the software object in the network computer NR to be transferred is provided with a digital signature and in the work station computer AR a verification takes place before utilization. This could uncover falsification of the object during the network transmission.

150: In the next step on the work station computer AR the SCV program 22 determines the type of use determined in conjunction with the USC parameters and becomes active accordingly. For example, if the parameter "acquisition of number of downloads" is set, an object-related counter application on the chip card, for example 13a in Figure 2, is activated and the counter incremented. Counting processes on the chip card are usefully carried out in the customary manner under cryptographic security.

160: The user recognizes after the download based on the list ASL on the screen which software is locally present and can trigger the start by clicking.

170: Thereby simultaneously - if the corresponding USC parameter is set - the usage time acquisition is triggered by the SCV and the usage time during the active utilization is periodically acquired thereby that the SCV program 22 from time to time (parameterizable) increments an object-related time counter on the chip card, for example 13b in Figure 2.

180: After termination of the use of a loaded software object on the work station computer AR, the SCV program 22, based on the delete mode parameter, decides whether or not the program is being deleted or stored on the work station computer AR.

190: Usage acquisition feedback to the VR is either triggered through the expiration

of the time interval parameter of a certificate USC or by the expiration of a time interval in the SCV program 22. In the case of the certificate triggering only the object-related acquisition data belonging to the particular certificate USC are affected, in the SCV trigger case the acquisition data of all certificates USC. Accordingly, the associated download counter and usage time counter are selected from the chip card 10.

195/230: After the customary mutual authentication between work station computer AR and administration computer VR, the selected counter counts are transferred to the administration computer VR.

240: In the administration computer VR the corresponding acquisition data are evaluated by means of the SUC program 42 and entered into the data base 46.

After pulling the chip card, a dialog box is displayed with the warning that the program will be deleted after a specific length of time (parameterizable), if the card is not inserted again.

Through the central administration of the rights of use and usage acquisition parameters in the administration computer VR, the described method makes possible a network-wide uniform and flexibly adaptable software distribution and utilization. Nevertheless it is possible for the user to change or even determine individual parameters if a corresponding USC parameter permits this degree of freedom. For example, the user can decide on his own the deletion or storage of a program after he has used it.

In the case of changes of individual USC parameters by the user, the original integrity-protected certificate USC remains unchanged, whereby it is ensured that with repeated downloads an integrity verification can be carried out.

The functionality can be expanded thereby that an automatic download through the SCV program 22 is triggered for the case that a software object during the execution calls up another software object, for example OLE technique, which is not available on the work station computer AR, whose identity, however, can be determined in one of the certificates USC.

The user in a network can apply the method from any computer connected to the network, if he can operate his individual authorization and acquisition chip card on this computer. In the case of a computer change, it is only necessary that before the first download of a software object he communicate with the administration computer in order to have issued the current rights according to the above described method.

With advancing chip card technology the html page with the list ASL and the SCV program can be stored on the chip card and be run. In this case communication with the VR is superfluous in the event of a computer change.

From the point of view of the user the method can also be applied to different networks independent of one another, for example Intranet for rights of use within the own company, Extranet for computers in a partner company, Internet for rights to worldwide use. This can take place with one and the same or with separate chip cards. When using the same chip card, separate keys for the different administration computers VR must be available.

An expansion of the method is also possible thereby that mechanisms for copy protection are incorporated into the described method. For this purpose for software objects which are to be copy-protected, using the public key of the user a so-called "key file" is generated, which the user receives after the download of the software object. Only with this "key file" and using the private key of the user can the software object be utilized.

By defining a USC parameter "copy-protected" and expanding the functions of the SCV program for the required communication between work station computer AR and administration computer NR as well as work station computer AR and chip card 10 according to the methods defined for copy protection, the copy protection can be integrated simply into the method explained here.

For the method, moreover, multifunctional chip cards can be used, which, for example, also are applied for other network applications. A combination with applications for identification in the network is preferably reasonable. Such applications can be, for example, www client authentication relative to an Internet server, www client identification in the case of mail (for example S/MIME) or www client identification for permission for access rights to network resources.

The method can generally also be applied - with low security requirements - without the use of chip cards. The keys and counters disposed on the chip card can, for example, also be carried on a disk (for example encrypted with a password), and the operations carried out on the chip card could be assumed by the SCV program 22.

Patent Claims

1. Method for controlling the distribution and utilization of data collections or programs denoted as software objects with computers (AR) coupled across a data network (30), which are administered at a central location (NR) and, upon request, are temporarily made available for use to the particular requesting computer (AR), wherein

   - the rights of use are developed in the form of user-specific certificates (USC), which are issued as a link between the authorizations and the authorization identification allocated to the software objects;
   - upon each request for a software object to the central administration instance (VR), the certificates (USC) are in each instance transferred user-related to the requesting computer (AR);
   - the certificates (USC) before the utilization of the software objects are verified by means of a personal data medium (10) and the usage is acquired on the same data medium (10);
   - a separate control program (SCV program 22) in the requesting computer (AR) on the basis of the rights of use controls the actions involving the software object and reports the status reports to the central site (NR).

2. Method as claimed in claim 1, in which the control program (SCV) is transferred from the central site (NR) to the requesting computer (AR) and is verified by means of the personal data medium (10) before its use.

3. Method as claimed in one of claims 1 or 2, in which the user-specific certificates (USC) are stored on the data medium (10) developed as a chip card.

4. Method as claimed in claim 3, in which the control program (SCV) resides in the data medium (10) and is, at least partially, executed there.

5. Method as claimed in one of claims 1 to 4, in which the data medium (10) can be coupled with any desired computers (AR) of the data network (30).

6. Method as claimed in one of claims 1 to 5, in which the control program (SCV) is checked as to whether or not requested software objects are already available on the computer (AR) and, in the event the result is positive, initiates the local provision of the software object.

7. Method as claimed in one of claims 1 to 6, in which, after the transfer of the certificates (USC), an index of the software objects corresponding to the certificates is displayed on the screen of the requesting computer (AR) and the request for the particular desired software object is triggered by the user.

8. Method as claimed in one of claims 1 to 7, in which the provision of the software objects can take place through different computers (NR) in the network (30).

9. Method as claimed in one of claims 1 to 8, in which control parameters comprised in the certificates (USC) can be changed by the user without an existing integrity protection being lost.

10. Method as claimed in one of claims 1 to 9, in which a further program, which is denoted in one of the present certificates (USC), called up as software object during the running of a program, is automatically requested through the separate control program (22) and thereupon transferred to the computer (AR) making the request.

11. Method as claimed in one of claims 1 to 10, in which the deletion of software objects takes place automatically after termination of its utilization.

12. Method as claimed in one of claims 1 to 11, in which the certificates (USC) comprise data regarding the type of acquisition of the usage extent of the software objects transferred to a requesting computer (AR) and that the separate control program (22) on the basis of these data controls the acquisition of the extent of the usage.

13. Method as claimed in claim 12, in which the utilization extent takes place by counting the transferred software objects.

14. Method as claimed in claim 12, characterized in that the [determination of the] extent of usage takes place by counting periodically recurring clock pulses.

15. Method as claimed in one of claims 12 to 14, in which the acquisition of the data regarding the usage extent takes place on the data medium (10).

16. Method as claimed in one of claims 1 to 15, in which in data networks (30) with several independent administration instances (VR) for software objects each administration instance issues utilization certificates (USC) for the software objects belonging to its area of competence.

17. Method as claimed in one of claims 1 to 16, in which all establishments of connections in the data network (30) and transfers take place under the security of keys.

18. Method as claimed in claim 17, in which the keys are contained on the data medium (10).

19. Method as claimed in one of claims 1 to 18, characterized in that software objects subject to copy protection are secured against copying through additional control parameters in the associated certificate (USC) and corresponding control functions in the separate control program (22).

**AMENDED SHEET (RULE (91)
ISA/EP**